Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application.

1-9.   (Canceled)

10.   (Currently amended) A method for providing access to a secured document item, comprising:

authenticating a user having credential information to a first server at a first location having the secured document itemstored therein; and

preventing access to a second server having the secured item stored therein while the user is accessing the first server from a first location; and

upon receiving [[an]]a request for access to the secured document request from the user to access the at a second server from at a second location, authenticating the credential information user to the second server, and disconnecting the user from the first server before establishing a connection that allows the user to access to the secured document at the second server.

11.   (Currently amended) The method as recited in claim 10, wherein the authenticating a user having credential information comprises authenticating both the credential information user and a client machine being used by the user.

- 5 -

HILDEBRAND *et al.*
Reply to Office Action of September 24, 2009   Appl. No. 10/076,181

12.   (Currently amended) The method as recited in claim 10, wherein the first

and the second servers are access points ~~for the user~~ to gain access to the secured

<u>document</u>~~item~~.

13.   (Currently amended) The method as recited in claim 29, wherein:

~~when the user~~ <u>in response to receiving a request for access to the secured</u>

<u>document</u> [[is]] at the first location, the <u>first server</u> ~~user~~ interacts over a network

with the <u>user</u>~~first server~~, and

~~when the user~~ <u>in response to receiving a request for access to the secured</u>

<u>document</u> [[is]] at the second location, the ~~user~~ <u>second server</u> interacts over a

network with the <u>user</u> ~~second server~~ using a second client machine at the second

location.

14.   (Currently amended) The method as recited in claim 10, further

comprising:

determining, prior to disconnecting the user from the first server, whether

~~the user~~ <u>access to the secured document</u> is permitted ~~to gain access through~~ <u>from</u>

the second location ~~to the secured item~~ <u>via the second server</u>.

15.   (Currently amended) The method as recited in claim 29, wherein the

authenticating the ~~user~~ <u>credential information to</u> ~~with~~ the first server occurs <u>in response</u>

<u>to receiving a</u> ~~while the~~ <u>request for access to the secured document</u>~~user is~~ at the first

location, and wherein the receiving the ~~access~~ request<u>for access via the second server</u>

occurs in response to receiving a request a request for access to the secured document

~~while the user is~~ at the second location.

16.   (Currently amended) The method as recited in claim 17, wherein the

authenticating the ~~user~~ credential information to the second server further comprises:

upon receiving the ~~access~~ request for access to access the secured

document ~~item~~ via the second server, determining permitted locations from which

the ~~user is permitted to access the~~ secured ~~item~~ document is permitted to be

accessed from;

determining whether the second location is one of the permitted locations

~~for the user~~; and

bypassing the disconnecting the user from the first server in response to

the ~~determination~~ determining that the second location is not one of the permitted

locations ~~for the user~~.

17.   (Currently amended) The method as recited in claim 30, wherein:

~~when the user~~ in response to receiving a request for access to the secured

document [[is]] at the first location, the first server ~~user~~ interacts over a network

with the user ~~first server~~ using a first client machine at the first location, and

~~when the user~~ in response to receiving a request for access to the secured

document [[is]] at the second location, the second server ~~user~~ interacts over a

network with the user ~~second server~~ using a second client machine at the second

location.

18.   (Currently amended) ~~A tangible~~ An article of manufacture including a computer-readable medium having instructions stored thereon, ~~computer-executable instructions~~ that, if executed by a computing device, cause the computing device to perform operations ~~a method,~~ comprising:

authenticating a user having credential information to a first server having a secured document ~~item~~ stored therein; and

~~preventing access to a second server having the secured item stored therein while the user is accessing the first server from a first location; and~~

upon receiving ~~an access~~ a request for access to the secured document ~~from the user to access the~~ at a second server from a second location, authenticating the ~~user~~ credential information to the second server, and disconnecting the user from the first server before establishing a connection that allows ~~the user to~~ access to the secured document at the second server.

19.   (Currently amended) The ~~tangible computer-readable medium~~ article of manufacture as recited in claim 31, wherein:

~~when the user~~ in response to receiving a request for access to the secured document [[is]] at the first location, the first server ~~user~~ interacts over a network with the user ~~first server~~, and

~~when the user~~ in response to receiving a request for access to the secured document [[is]] at the second location, the second server ~~user~~ interacts over a

network with the user ~~second server~~ using a second client machine at the second

location.

20.   (Currently amended) The ~~tangible computer-readable medium~~ article of

manufacture as recited in claim 32, the operations further comprising:

determining, prior to the reconfiguring of either the first local module at

the first server or the second local module at the second server, whether the user

having the credential information is permitted to ~~gain~~ access the secured

document from the second location ~~to the secured item~~ via the second server.

21.   (Currently amended) A system for controlling access to a secured

document ~~item~~, comprising:

an access control device, ~~wherein the access control device authenticates~~

configured to:

authenticate a user having credential information to a first server having

the secured document ~~item~~ stored therein, ~~and prevents access to a second server~~

~~machine while the user is accessing the first server from a first location,~~ ; and[[,]]

upon receiving [[an]]a request for access to the secured document ~~request~~

~~from the user to access the~~ at a second server from a second location, authenticate

~~authenticates~~ the ~~user~~ credential information to the second server, and disconnect

~~disconnects~~ the user from the first server before establishing a connection that

allows ~~the user to~~ access to the secured document at the second server.

Atty. Dkt. No. 2222.5390002

- 9 -
HILDEBRAND *et al.*
Reply to Office Action of September 24, 2009
Appl. No. 10/076,181

22. (Currently amended) The ~~tangible computer-readable medium~~ article of manufacture as recited in claim 31, wherein authenticating the ~~user~~ credential information comprises authenticating both the ~~user~~ credential information and a client machine ~~being used by the user~~.

23. (Currently amended) The ~~tangible computer-readable medium~~ article of manufacture as recited in claim 32, the operations further comprising:

determining, prior to the reconfiguring the first local module at the first server and the second local module at the second server, whether the user having the credential information is permitted to ~~gain~~ access to the secured document from the second location ~~to the secured item~~ via the second server.

24. (Currently amended) The ~~tangible computer-readable medium~~ article of manufacture as recited in claim 33, wherein the authenticating the ~~user~~ credential information to the second server further comprises:

upon receiving the ~~access~~ request [[to]]for access to the secured document~~item~~ via the second server, determining permitted locations from which the ~~user~~ secured document is permitted to be accessed from~~gain access to the secured item~~;

determining whether the second location is one of the permitted locations ~~for the user~~; and

- 10 -
Reply to Office Action of September 24, 2009
HILDEBRAND *et al.*
Appl. No. 10/076,181

bypassing the disconnecting the user from the first server in response to

the determination that the second location is not one of the permitted locations for

~~the user~~.

25.   (Currently amended) The system as recited in claim 21, wherein the

access control device is further configured to authenticate ~~authenticates~~ both the ~~user~~

credential information and a client machine ~~being used by the user~~.

26.   (Currently amended) The system as recited in claim 21, wherein the first

and the second servers are access points ~~for the user~~ to gain access to the secured

document ~~item~~.

27.   (Currently amended) The system as recited in claim 35, wherein the

access control device is further configured to determine ~~determines~~, prior to

reconfiguring the first local module at the first server and the second local module at the

second server, whether ~~the user is permitted to gain~~ access to the secured document is

permitted from the second location ~~to the secured item~~ via the second server.

28.   (Canceled)

29.   (Currently amended) The method as recited in claim 10, further

comprising:

        authenticating the ~~user~~ credential information to ~~with~~ the first server with

respect to a previous ~~access~~ request for access;

subsequently receiving the ~~access~~ request _for access_ via the second server; and

authenticating the ~~user~~ _credential information to_ ~~with~~ the second server with respect to the ~~access~~ request _for access_.

30.   (Currently amended) The method as recited in claim 29, wherein the disconnecting the user from the first server comprises:

upon receiving the ~~access~~ request _for access_ via the second server, identifying a first local module previously supporting _a connection from_ ~~the user~~ ~~at~~ the first server;

reconfiguring the first local module at the first server to remove support for _access to the secured document_ ~~the user~~ at the first server;

identifying a second local module to support _access to the secured document_ ~~the user~~ at the second server; and

reconfiguring the second local module at the second server to add support for _access to the secured document_ ~~the user~~ at the second server.

31.   (Currently amended) The ~~tangible computer-readable medium~~ _article of manufacture_ as recited in claim 18, _the operations_ further comprising:

authenticating the ~~user~~ _credential information to_ ~~with~~ the first server with respect to a previous ~~access~~ request _for access_;

subsequently receiving the ~~access~~ request _for access_ via the second server; and

authenticating the ~~user~~ the credential information to ~~with~~ the second

server with respect to the ~~access~~ request for access.

32.   (Currently amended) The ~~tangible computer-readable medium~~ article of

manufacture as recited in claim 31, wherein the disconnecting the user from the first

server comprises:

upon receiving the ~~access~~ request for access via the second server,

identifying a first local module previously supporting access to the secured

document ~~the user~~ at the first server;

reconfiguring the first local module at the first server to remove support

for access to the secured document ~~the user~~ at the first server;

identifying a second local module to support access to the secured

document ~~the user~~ at the second server; and

reconfiguring the second local module at the second server to add support

for access to the secured document ~~the user~~ at the second server.

33.   (Currently amended) The ~~tangible computer-readable medium~~ article of

manufacture as recited in claim 32, wherein:

~~when the user~~ in response to receiving a request for access to the secured

document [[is]] at the first location, the first server ~~user~~ interacts over a network

with the user ~~first server~~ using a first client machine at the first location, and

~~when the user~~ in response to receiving a request for access to the secured

document [[is]] at the second location, the second server ~~user~~ interacts over a

network with the <u>user</u> ~~second~~ server using a second client machine at the second

location.

34.   (Currently amended) The system as recited in claim 21, wherein the

access control device <u>is further configured to</u>:

~~authenticates~~ <u>authenticate</u> the <u>credential information to</u> ~~user with~~ the first

server with respect to a pervious ~~access~~ request <u>for access</u>;

subsequently <u>receive</u> ~~receives~~ the ~~access~~ request <u>for access</u> via the second

server; and

~~authenticates~~ <u>authenticate</u> the <u>credential information to</u> ~~user with~~ the

second server with respect to the ~~access~~ request <u>for access</u>.

35.   (Currently amended) The system as recited in claim 34, wherein the

access control device <u>is further configured to</u>:

~~identifies~~ <u>identify</u> a first local module previously supporting the ~~user~~

<u>client machine</u> at the first server upon receiving the ~~access~~ request <u>for access</u> to

~~access~~ the <u>secured document</u> ~~secure item~~ via the second server;

~~reconfigures~~ <u>reconfigure</u> the first local module at the first server to

remove support for ~~the user~~ <u>access to the secured document</u> at the first server;

~~identifies~~ <u>identify</u> a second local module to support ~~the user~~ <u>access to the</u>

<u>secured document</u> at the second server; and

~~reconfigures~~ <u>reconfigure</u> the second local module at the second server to

add support for ~~the user~~ <u>access to the secured document</u> at the second server.